U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

February 25, 2019

TO: Republican Members, Subcommittee on Consumer Protection and Commerce

FROM: Republican Committee Staff

RE: Hearing entitled "Protecting Consumer Privacy in the Era of Big Data." February 26, 2019 at 10:00 a.m. in 2123 Rayburn House Office Building.

I. WITNESSES

- **Republican Witness:** Roslyn Layton, PhD, Visiting Scholar, American Enterprise Institute;
- **Bipartisan Witness:** Dave Grimaldi, Executive Vice President for Public Policy, IAB;
- **Bipartisan Witness:** Denise Zheng, Vice President, Technology, Innovation, Business Roundtable;
- **Democrat Witness:** Brandi Collins, Senior Campaign Director, Media, Democracy & Economic Justice, Color of Change; and
- **Democrat Witness:** Nuala O'Connor, President and CEO, Center for Democracy & Technology.

II. BACKGROUND

According to a recent National Telecommunications and Information Administration survey, most Americans have privacy and security concerns online. Roughly 73 percent of American households' report privacy and security concerns online and about 33 percent of those households do not participate in certain online activities due to those concerns.[1] Some of these concerns can be attributed to a lack of transparency and understanding of how companies collect, use, and share consumer information online. According to stakeholders recently surveyed by the Government Accountability Office, companies' privacy policies contribute to this lack of

[1] https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds

understanding.[2] Often, these policies contain technical provisions and legalese, are difficult to locate, or may be too long for consumers to digest easily.[3]

In the U.S., privacy has a key place in our founding principles and documents, notably in the Bill of Rights. Further, commercial privacy laws have been historically designed around specific harms presented by the misuse of sensitive data categories or particularly at-risk populations, including children.[4] There are a number of federal sector-specific privacy laws, and with general enforcement authority the Federal Trade Commission (FTC) ensures companies do not use unfair or deceptive acts or practices in commerce.

In the European Union, the General Data Protection Regulation (GDPR) entered in to force in May 2016 after four years of negotiations, and two years later in May 2018 became enforceable. California followed suit with the passage of the California Consumer Privacy Act (CCPA) of 2018 in June 2018.[5] Industry calls for a single federal privacy bill increased after the California privacy law passed and the subsequent introduction of a number of varying privacy bills in other states.[6] This memorandum summarizes some developments in privacy law and enforcement from the Fair Information Practice Principles (FIPPs) and the OECD Guidelines to the European Union's GDPR, the California Privacy Protection Act of 2018, and the current status of federal activities relating to privacy as all of these efforts will be informative to the debate around federal privacy legislation.[7]

III. FAIR INFORMATION PRACTICE PRINCIPLES & OECD GUIDELINES

The FIPPs were developed in the U.S. in the 1970s around the basic principles of notice, choice, access, and security. The FIPPs underpin other privacy frameworks including OECD Guidelines first released in 1980 and subsequently updated,[8] the APEC Privacy Framework,[9] the

---

[2] https://www.gao.gov/assets/700/696446.pdf
[3] *Id*. at 18.
[4] https://www.gao.gov/assets/700/696446.pdf at 6.
[5] California AB 375 was introduced on June 21, 2018 and was signed into law on June 28, 2018. An amendment measure was signed into law in August 2018.
[6] *See* https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy; http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376.pdf
[7] Terminology reflected in the summary reflects language used in the relevant documents.
[8] http://www.oecd.org/sti/ieconomy/privacy.htm; https://www.cov.com/~/media/files/corporate/publications/2013/10/what_does_the_revision_of_the_oecd_privacy_guidelines_mean_for_businesses.pdf
[9] https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015); *see also* https://www.apec.org/Publications/2016/11/Enabling-Legal-Compliance--CrossBorder-Data-Transfers-with-the-APEC-CrossBorder-Privacy-Rules-CBPR

National Institute of Standards and Technology (NIST) Special Publication 800-53 Appendix J,[10] and privacy laws around the world. The OECD principles state:

- Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject.

- Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

- Purpose Specification Principle: The purposes for which personal data re collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such other as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except (a) with the consent of the data subject; or by the authority of law.

- Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

- Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- Individual Participation Principle: Individuals should have the right (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; (b) to have communicated to them, data relating to them within a reasonable time, at a charge, if any, that is not excessive in a reasonable manner, and in a form that is readily intelligible to them; (c) to be given reasons if a request is denied, and to be able to challenge such denial; and (d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed, or amended.

[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles above.[11]

IV. GENERAL DATA PROTECTION REGULATION

The stated objectives of the European Union's GDPR are to "lay[ ] down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data" and to "protect[ ] fundamental rights and freedoms of natural personal and in particular their right to the protection of personal data."[12] GDPR applies to "the processing of personal data wholly or partly by automated means and to the process other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."[13] GDPR supersedes the Data Protection Directive of 1995, and Member State implementing laws under the Directive, setting one standard for the European Union. Under GDPR, Europeans are guaranteed the following rights:

- **Right to be informed:** at the time your personal data is being collected, you have the right to know why it is being collected, the legal basis for processing it, retention periods, and who it will be shared with;

- **Right of access:** the right to know whether your personal data is being processed and the right to request of copy of your personal information;

- **Right to rectification:** the right to demand inaccurate personal information be corrected and incomplete information be completed;

- **Right to be forgotten:** the right to demand your personal information be permanently deleted by a controller;

- **Right to be notified:** a controller must, without delay, notify you if your personal information was compromised in a data breach;

- **Right to restrict data processing:** the right to prevent companies from processing your personal information;

- **Right to data portability:** the right to obtain, copy, move, or otherwise transfer your personal information to a new, different controller or for your own personal means;

- **Right to object:** the right to object to the processing of your personal information under certain circumstances, such as for direct marketing;

---

[11] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[12] https://gdpr-info.eu/art-1-gdpr/
[13] https://gdpr-info.eu/art-2-gdpr/

- **Right to not be subject to automated decision making:** you have the right to not be subject to decisions made by automated individual decision making, such as profiling;

- **Right to withdraw consent:** you must be informed of your right of withdrawal before giving your consent and have the ability to withdraw that consent at any time;

- **Right to a remedy:** if your personal information is processed or otherwise used in violation of GDPR, you may file a complaint and seek a remedy; and

- **Right to representation:** you have the right to mandate a not-for-profit body or similar organization exercise your rights on your behalf.[14]

A. Personal Data

Personal data is the threshold for whether the obligations and rights under GDPR are invoked. Pursuant to Art. 4(1), personal data means: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[15] Because GDPR defines personal data as "any information" it is understood to be broad.

B. Right to Be Forgotten & Enforcement

The right to be forgotten grants Europeans the ability to request their personal information be permanently deleted by a controller. This right originally derives from the case *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014). In the case, Mr. Costeja González, a Spanish national, filed a complaint with the Spanish Data Protection Agency against La Vanguardia Ediciones SL, a daily Spanish newspaper, and Google Spain and Google, Inc.[16] Mr. Costeja González's complaint was based on the fact that when someone Googled him, they could find an announcement for a real-estate auction related to the collection of certain debts owed by him.[17] Mr. Costeja González demanded that Google either remove or alter the pages in question and that they be required to remove or conceal any personal data related to him so that he no longer appeared in search results or La Vanguardia, the newspaper in question.[18]

The AEPD granted Mr. Costeja González's request, finding that Google had to take necessary measures to "withdraw the data from their index and to render access to the data

[14] Chapter 3, Arts. 12-23
[15] https://gdpr-info.eu/art-4-gdpr/
[16] https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf
[17] *Id.*
[18] *Id.*

impossible in the future."[19] As a result, Google brought two actions in the national high court of Spain requesting the decision be overturned. The national high court then requested the European Court of Justice to weigh in. Among other findings, the European Court of Justice held that Google had to honor Mr. Costeja González's request that "links to web pages be removed" from search results because "he wishes the information appearing on those pages relating to him personally" be forgotten and that any linked web pages "be removed from such a list of results" related to Mr. Costeja Gonzalez.[20]

GDPR codified the European Court of Justice's holding that consumers enjoy the right to be forgotten. Under GDPR, personal data must be erased immediately "where the data are no longer needed for their original processing purpose, or the data subject has withdrawn his consent and there is no other legal ground for processing, the data subject has objected and there are no overriding legitimate grounds for the processing, or erasure is required to fulfill a statutory obligation" under law.[21] Other examples of GDPR enforcement are limited at this time.

There are two tiers of penalties for violations of GDPR: first, up to 10 million EUR (or about $11 million USD) or two-percent of the worldwide annual revenue of the prior financial year, whichever is higher;[22] and second, 20 million EUR (or about $22 million USD) or four-percent of the worldwide annual revenue of the prior financial year, whichever is higher.[23] Penalties are levied by individual Member States after considering the following: nature of infringement; intention; mitigation; preventative measures; history; cooperation; data type; notification; certification; and other aggravating or mitigating circumstances.[24]

On January 21, 2019, $57 million in fines was accounted against Google by CNIL, France's data protector regulator, for failure to comply with GDPR.[25] According to CNIL, Google failed to provide enough information to users about its data consent policies and did not give them enough control over how their information is used.[26]

D. Compliance Costs

According to Forbes, compliance with GDPR cost large British firms a combined $1.1 billion and American companies approximately $7.8 billion.[27] On average, GDPR cost the

---

[19] *Id.*
[20] *Id.* at 3.
[21] https://gdpr-info.eu/issues/right-to-be-forgotten/
[22] Violators of the following articles may be subject to this penalty: controllers and processors under Articles 8, 11, 25-39, 42, 43; certification body under Articles 42, 43; monitoring body under Article 41(4).
[23] Violators of the following articles may be subject to this penalty: the basic principles for processing, including conditions for consent, under Articles 5, 6, 7, and 9; the data subjects' rights under Articles 12-22; the transfer of personal data to a recipient in a third country or an international organization under Articles 44-49; any obligations pursuant to Member State law adopted under Chapter IX; any non-compliance with an order by a supervisory authority (83.6).
[24] https://www.gdpreu.org/compliance/fines-and-penalties/
[25] https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil
[26] *Id.*
[27] https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#708ca0c34a22

Fortune 500 companies an average of $16 million.[28] GDPR requires larger companies hire a data protection officer that can cost on average a salary of $71,000 to $354,000, depending on the size of the company.[29]

Data indicates GDPR has resulted in larger companies gaining market share as well as driving out some American companies from Europe altogether. For example, a review of data regarding digital advertising from pre-GDPR in April to post-GDPR in July 2018, shows that smaller advertising firms lost between 18 percent and 31 percent, whereas Google has increased its market share.[30] Since GDPR went into effect over 1,000 news sites have gone completely dark in Europe.[31] Specifically, EU residents can no longer access Tribune Publishing media, whose flagship newspapers include the Los Angeles Times, the Chicago Tribune, New York Daily News, the Hartford Courant (America's longest running newspaper since 1764), the Orlando Sentinel, and the Baltimore Sun" and "more than 60 newspapers of Lee Enterprises covering news across 20 U.S. states."[32]

V. CALIFORNIA CONSUMER PRIVACY ACT

On June 21, 2018, AB-375 was introduced by Representatives Chau and Hertzberg,[33] and on June 28, 2018, Governor Jerry Brown signed CCPA into law.[34] On August 31, 2018, the California State Legislature passed SB-1121 to make amendments to the law and delay its implementation until January 1, 2020.[35] The enforcement date is the first of either July 1, 2020, or six months after implementing regulations are finalized. The law contains the following provisions, among others:

- Grant a consumer a right to request a business disclose the personal information collected about the consumer, the categories of sources from which the information is collected, the business purpose for the collection or selling of that information, and the categories of third parties the information is shared with;

- Grant a consumer the right to request deletion of personal information, with some exceptions;

- Grant a consumer a right to request that a business that sells the consumer's personal information, or discloses it for a business purpose, disclose the categories of

---

[28] *Id.*
[29] *Id.*
[30] https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr
[31] https://fedsoc.org/commentary/publications/the-gdpr-what-it-really-does-and-how-the-u-s-can-chart-a-better-course
[32] *Id.; see also* http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/
[33] https://www.wired.com/story/new-privacy-bill-could-give-californians-unprecedented-control-over-data/?intcid=inline_amp&_gl=1*159snfb*_ga*YW1wLW5Qck9wZXlmeU8zYS1USTFtRkhCcjJNb2xsZ2pZenFMdUFJYmR0UUxmNUE2S0RCX0hiaDQ0b1lwaHNweGstbHY
[34] https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180AB375
[35] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

information that it collects and categories of information and the identity of third parties to which the information was sold or disclosed;

- Grant a consumer the ability to opt out of the sale of personal information by a business and prohibit the business from discriminating against the consumer for exercising this right, including by charging the consumer who opts out a different price or quality of goods and services with certain exceptions;

- Prohibit a business from selling personal information of consumers under the age of 16, unless affirmatively authorized;

- Provide of its enforcement by the Attorney General of California; and

- Provide a private right of action in connect with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information.[36]

A. Personal Information

Under CCPA, personal information is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[37] Meaning, data may be protected under the Act even if it does not relate specifically to a single individual.[38] For example, this includes "Internet Protocol addresses…browsing history, search history," "commercial information, including…purchasing or consuming histories or tendencies," and "inferences drawn from any of the information" identified to a consumer or household with respect to "preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[39]

B. Enforcement

Under CCPA, any business or third party can seek the opinion of the California Attorney General for guidance on complying with the Act. However, if a business is in violation of the Act and fails to cure any violation within 30 days of being notified, that business may be "subject to an injunction and…a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation."[40] Additionally, CCPA offers a limited private right of action. Specifically, if any consumer's non-encrypted or non-redacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure because a business failed to implement and maintain

[36] CCPA Legislative Counsel's Digest found here: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
[37] Cal. Civ. Code § 1798.140(o)(1)
[38] https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/
[39] Cal. Civ. Code § 1798.140(o)(1)(A), (D), and (K)
[40] Cal Civ. Code § 1798.155(a) and (b)

reasonable data security practices, then a private right of action may be filed to "recover damages in an amount of not less than one hundred dollars ($100) and not greater than seven hundred and fifty dollars ($750) per consumer per incident."[41]

VI. FEDERAL TRADE COMMISSION & OTHER FEDERAL ACTIVITIES

The Federal Trade Commission (FTC) is the primary law enforcement agency charged with preventing the majority of commerce from using unfair or deceptive acts or practices.[42] An act or practice is "unfair" if it causes, or is likely to cause, substantial injury not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition as a result of the practice.[43] An act or practice is "deceptive" if it is material and is likely to mislead consumers acting reasonably under the circumstances. The FTC has applied this authority where deceptions or violations of written privacy policies and representations of data security have occurred.[44]

Additionally, the FTC has authority to enforce a variety of sector specific laws, including the Gramm-Leach-Bliley Act (GLBA), Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act (COPPA), the Equal Credit Opportunity Act, the Fair Credit Reporting Act (FCRA), the Fair Debt Collection Practices Act, and the Telemarking and Consumer Fraud and Abuse Prevention Act. As of January 2018, the FTC has brought enforcement actions addressing a number privacy and data security issues, which includes over 130 spam and spyware cases, more than 50 general privacy actions, more than 60 data security cases, more than 30 cases under GLBA, and more than 20 cases under COPPA.[45]

FTC actions generally result in a settlement where the parties agree to terms laid out in a consent decree. These settlement agreements typically require a company to: implement reasonable privacy and security programs; subject the company to long-term monitoring of compliance, generally 20 years; provide monetary redress to consumers; forfeit any money gained from the unfair or deceptive conduct; delete illegally obtained consumer information; and provide increased transparency and choice mechanisms to consumers.[46] If a company violates the terms of the consent decree, the FTC can then levy civil penalties.[47]

---

[41] Cal Civ. Code § 1798.154(a)(1)(A)
[42] 15 U.S.C. § 45(a)(1)
[43] https://www.gao.gov/assets/700/696437.pdf at 9.
[44] In 2011, the FTC settled with Facebook over charges that Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public." https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep
[45] https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf; for a list of all privacy and data security related cases, please visit https://www.ftc.gov/enforcement/cases-proceedings/terms/245%2B247%2B249%2B262
[46] https://www.gao.gov/assets/700/696437.pdf at 10.
[47] *Id.*

The FTC is currently conducting a series of workshops on issues within its jurisdiction, several focusing on consumer protection issues including privacy and data security, "Hearings on Competition and Consumer Protection in the 21st Century."[48]

In September 2018, the National Telecommunications and Information Administration announced a request for comment period on "ways to advance consumer privacy while protecting prosperity and innovation."[49] There were over two hundred submissions to the request for comments.[50]

VII. STAFF CONTACTS

Please contact Melissa Froelich or Bijan (BJ) Koohmaraie of the Republican Committee staff at (202) 225-3641 with questions.

[48] https://www.ftc.gov/policy/hearings-competition-consumer-protection
[49] https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf
[50] https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy